NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

WINDOWS NT THREATS AND VULNERABILITIES

by

Febbie P. Moore

September, 1997

Thesis Advisor: Norman Schneidewind

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 1997	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. WINDOWS NT THREATS AND VULNERABILITIES		5. FUNDING NUMBERS	
6. AUTHOR(S) Febbie P. Moore			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

The objective of this research is to examine the threats and vulnerabilities of a Windows NT network. One aspect of this research is to add to the Department of Defense's understanding of the disadvantages of the system. This research demonstrates five vulnerabilities of Windows NT with respect to the military network operating system security environment. First, there is the NetBIOS-over-TCP/IP vulnerability. Windows NT by default allows networking over this protocol. This protocol could allow an attacker to remotely connect to a drive and edit the registry. Second, the server message block (SMB) vulnerability allows remote access to shared directories. An unauthorized user could use this hole to access everything on the shared resources. Third, the remote registry access vulnerability could allow an attacker to view and change the contents of another computer's Registry. Fourth, improperly set permissions could allow unauthorized access to sensitive and classified data. Fifth, the built-in file transfer protocol (FTP) service allows users to change directories. Users could use this hole to see the root directory. Before DOD becomes too committed to Windows NT, these issues need to be addressed.

14. SUBJECT TERMS Windows NT, Threats, Vulnerabilities			15. NUMBER OF PAGES 74
			16. PRICE CODE
17. SECURITY CLASSIFICA- TION OF REPORT Unclassified	18. SECURITY CLASSIFI- CATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICA- TION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

WINDOWS NT THREATS AND VULNERABILITIES

Febbie P. Moore
Lieutenant, United States Navy
B.A., University of Mississippi, 1990

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN
INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September, 1997

ABSTRACT

The objective of this research is to examine the threats and vulnerabilities of a Windows NT network. One aspect of this research is to add to the Department of Defense's understanding of the disadvantages of the system. This research demonstrates five vulnerabilities of Windows NT with respect to the military network operating system securty environment. First, there is the NetBIOS-over-TCP/IP vulnerability. Windows NT by default allows networking over this protocol. This protocol could allow an attacker to remotely connect to a drive and edit the registry. Second, the server message block (SMB) vulnerability allows remote access to shared directories. An unauthorized user could use this hole to access everything on the shared resources. Third, the remote registry access vulnerability could allow an attacker to view and change the contents of another computer's Registry. Fourth, improperly set permissions could allow unauthorized access to sensitive and classified data. Fifth, the built-in file transfer protocol (FTP) service allows users to change directories. Users could use this hole to see the root directory. Before DOD becomes too committed to Windows NT, these issues need to be addressed.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I. INTRODUCTION

A. PROBLEM DEFINITION

The purpose of this research is to examine the threats to and vulnerabilities of a Windows NT network. The primary objective is to offer solutions to Windows NT vulnerabilities.

B. MOTIVATION

The motivation behind this research is twofold. First, the U.S. Navy is in the process of heavily committing to Windows NT as its standard network operating system. Research about Windows NT will add to the Navy's and DOD's understanding of the advantages and disadvantages of the system. Secondly, since NPS is currently installing Windows NT technology into labs and departments, this research will add to NPS's students and staff understanding of the strengths and weaknesses of the network.

C. DOD

Networks are a special challenge to DOD. In the past when mainframes were in heavy use, physical computer security was easier to handle because computers operated in batch mode or were connected via hard lines. Since then, computers have moved to the desktop. As DOD strives to increase the information flow between its agencies through networks, it is faced with trying to solve the network security problem. The Department of Defense has an information infrastructure of over 10,000 local networks and 100 long-

distance networks [Stillman, Stephenson 96]. Examining the vulnerabilities of Windows NT and providing feedback to the Defense Information Systems Agency will help this agency to correctly evaluate the risks associated with Windows NT.

D.   THESIS ORGANIZATION

This thesis is organized in the following manner: Chapter II describes Security Terminology and Concepts, and threats to security. Chapter III examines DOD's security environment. Chapter IV details the vulnerabilities and threats researched in this thesis. Chapter V discusses the ways to secure a network and Chapter VI furnishes conclusions and recommendations.

There is one appendix to this thesis: a list of abbreviations and definitions.

II.   SECURITY

A.   INTRODUCTION

This chapter gives an overview of key security concepts and terminology and threats to security. In this chapter the standard definitions of threat, vulnerability, and risk are presented.

B.   SECURITY TERMINOLOGY

The rapid proliferation and inter-connection of computers has significantly worsened computer and network security problems.[Bace, Schaefer 95]. Once a network includes parts of the outside world, vulnerability increases. Networks present greater accessibility to attackers by providing more ways of breaching a system. The accessibility of networks provide numerous opportunities for information to be leaked or modified. The government needs connectivity with large networks, including the Internet, to support its IT21 strategy. The use of networks, especially the Internet, to enhance DOD's ability to communicate and share information has increased DOD's exposure to attack by providing unauthorized users a way to access DOD systems.

One way computer systems provide security is by controlling access. System access controls prevent unauthorized users from getting into a system by controlling access to the system through the use of passwords, protection of passwords and by tracking who is doing what in the system. The system tracks who is doing what in the system by the two step process of identification and authentication. Identification is the

user telling the system who he is and authentication is the user proving to the system that he is who he claims to be. Three ways a user can prove himself is through the use of passwords, electronic keys, or physiological traits (finger prints, hand print, retina pattern).

Data access controls tracks who can access what data, and for what purpose. Two types of access controls are discretionary access control (DAC) and mandatory access control (MAC).

Discretionary access control restricts access to system objects (files, directories, devices) based on the identity of the users and/or groups to which they belong. Discretionary means that a user with certain access permissions is capable of passing those permissions to another user [Russell, Gangemi 92].

Mandatory access control restricts access to system objects based on the sensitivity of the information in the object and the authorization of the subject (user clearance) to access information at that sensitivity level. Mandatory means that the system enforces the policy; users do not have the discretion to share their files [Russell, Gangemi 92].

C.   SECURITY CONCEPTS

To gain a basic understanding of computer security it is necessary to understand some of the concepts for computer security. There are three areas of computer security: confidentiality, accuracy and availability [Russell, Gangemi 92].

1. Confidentiality

Confidentiality is sometimes called secrecy, and it means not allowing unauthorized access to information . The confidentiality concept is a prime objective of DOD. Confidentiality is maintained by preventing unauthorized access to information under protection.

2. Accuracy

The accuracy or integrity concepts means the protection of information from unwanted changes, accidental or malicious [Russell, Gangemi 92]. An integrity attack is usually an attack that causes information to be modified in some way. Secure systems must have some way of preventing information from being compromised. Controlling access to information is just one way of protecting it from modification.

3. Availability

The availability concept means a user can access information when he needs to. Availability differs from the other two concepts of computer security. One difference is availability pertains to both information and resources. Secondly, the key objective of availability is the prevention of service denial, not access control [Abrams 95]. As networks are relied on more and more, availability becomes very important. Availability can be ensured to some extent by improved security counter measures, but it cannot be guaranteed. Availability consists of three areas: (1) The ability to access a specific resource within a specific time frame. (2) The ability to use or access objects and

5

resources as required. (3) The prevention of the unauthorized withholding of information or resources [Abrams 95].

User access convenience and security controls is a discipline of making trade- offs. Threats to computer security can be minimized by providing access control over information on a computer to ensure that only authorized users are allowed access.

Networks and systems are constantly being added. Many users of these systems do not realize the extent of the vulnerabilities of these systems. The current culture of open systems, free services and unlimited connectivity is opposite to security. Today most users have workstations or personal computers acting as terminals. A majority of these systems use login access, which is a key security vulnerability. Avoiding login access is a strong protection against unauthorized access. Login provides the most flexibility to remote users, but also the most risk. It is possible to reconcile these conflicting goals by making sure communications are secure. There are cryptographic solutions to this problem. Secondly, access mechanisms must be enforced and detection devices used. It is impossible to make any system absolutely secure, but it is possible to reduce the risk.

D.   THREATS TO SECURITY

A threat is the potential to cause harm to a network or a system. Some of the most common threats to security are disclosure, damage, theft and malicious software. A major threat to information security is disclosure.

1. Disclosure

Disclosure is basically the unintended release of information [Abrams 95]. The unintended release of information can result from poor user practices. Disclosure is a threat to the confidentiality of information. Information can be protected from unauthorized disclosure by using some form of a crypto system.

2. Damage

A threat to data integrity is the damage to information. One form of damage is the unauthorized modification of information [Abrams 95]. Damage also consists of deletion of data or programs or even the subtle alteration of information.

3. Theft

A threat to resources is theft. Theft can mean unauthorized utilization of resources, such as electronic mail or the out right stealing of resources such as illegally transferring money from one account to another.

4. Malicious Software

Malicious software is known by many names: Trojan horse, virus, worm, trap door, time/logic bombs etc. Malicious software is software used by an attacker to breach the security of a computer system or network for theft , disruption, disclosure or other

forms of computer misuse. Detailed descriptions of the above types of malicious software can be found in the Appendix.

E.   TYPES OF THREATS

Threats fall into three areas: natural, unintentional, and intentional.

1.   Natural

Natural or physical threats are threats that physically endanger facilities and equipment [Russell, Gangemi 92]. Fires, floods and power failures are some examples of physical disasters. These type of disasters are not always preventable. The damage these threats pose can be reduced by establishing policies that are geared toward preventing hazardous conditions. Also critical data should be backed up off-site in case a disaster occurs.

2.   Unintentional

Unintentional threats are usually the result of human error that leads to unauthorized disclosure. A user might inadvertently set the wrong access to files containing sensitive information, allowing information to be disclosed or modified. This type of human error leaves systems vulnerable to malicious users. The largest source of information loss is due to unintentional human actions during operations [OTA 94]. It has been estimated by some experts that over half the total financial and productivity losses in information systems is the result of unintentional human errors.

3. Intentional

Intentional threats are threats posed by hackers and other individual who deliberately set out to corrupt or access someone else's system or data. These individuals are either insiders or outsiders.

Many information security violations are performed by insiders who either engage in unauthorized activity or activity that exceed their authority. There are several types of insiders. The disgruntled employee might try to steal or try to cause damage by destroying records or files. The greedy employee who might use his access to steal corporate or customer funds. These individuals may be system administrators or just casual users who are willing to share a password. The most dangerous insider is the lazy or untrained, who does not bother to change passwords or set proper access permissions.

Outsiders consists of individuals from foreign intelligence agencies and hackers. Foreign intelligence agents are outsiders whose attacks are centered on classified information. Hackers are intruders who are usually more interested in the challenge of breaking-in than for monetary means. They break-in to defeat each new security challenge. Criminals on the other hand are usually interested in theft or other types of computer crime.

The most effective computer attacks or those accomplished by insiders and outsiders.

F. VULNERABILITIES

Vulnerabilities are weaknesses in a computer system. Threats are capable of exploiting a network's vulnerabilities. All computers and network systems are vulnerable to some form of attack. One objective of computer security is to identify the vulnerabilities. Below are some common vulnerabilities of most computer systems.

1. Physical Vulnerability: Buildings and computer rooms are susceptible to break-in, vandilization, and theft. Locks, guards and alarms provide a defense against break-ins.

2. Natural Vulnerability: Computers are susceptible to fire, power loss, water damage, and so on. A defense against these dangers is through preventive measures and detection. Some detection and preventive measures are: surge protectors, alternative power supply, sprinklers, fire and water detectors and sprinklers.

3. Hardware and Software Vulnerability: Hardware and software failures can bring a whole system down or open it to penetration. Hardware and software failures might cause memory protection features to fail. If the privileged and non-privileged memory is breached security holes could be opened in a system. A defense against this happening is to make sure hardware components are connected properly and software is installed correctly.

4. Communications Vulnerabilities: Computers attached to networks increase the risk of penetration into a system. Networks gives attackers more ways to access a system. Passwords can be stolen, messages can be intercepted, miss-routed and forged. You can protect against these vulnerabilities by installing firewalls and by using encryption devices.

5. Human Vulnerabilities: System administrator's lax security measures and ignorance[Russell, Gangemi 92]. A defense against this type of vulnerability is to ensure system administrators adhere to security requirements and that they are properly trained.

6. Malicious users: Individuals who attempt to penetrate information systems; browse, steal, modify data; deny access or service to authorized users; or cause damage or harm in some other way are considered malicious users. Defenses against the malicious user are monitoring systems, increasing user awareness and improving security procedures.

G.   RISK

The probability that a particular threat will exploit a particular vulnerability is risk [Fites, Kratz 93]. Risk assessment is the process that considers the threats to information and the loss that would occur if a threat were to occur. Risk assessments allows an organization to consider solutions to security problems which are cost-effective. The solutions may either attempt to reduce the probability of threats, lessen the effects of various threats, or aid in the recovery from a successful threat.   The ultimate goal of the assessment is to determine the computer facilities assets and their values; identify all potential security threats and their likelihood of occurrence; assess the vulnerability of systems and networks to the identified threats; and determine cost effective counter measures [Palmer, Potter 90].

Security is a tradeoff. Cost of a security mechanism or product must be balanced against the risk of not having it. A number of questions must be answered when

determining an organization's information assets and when considering how to protect them:

1. What information do you have and how important is it? Determine what information an organization has and assess how important that information is to the organization. Information important to you may have little value to another organization.

2. How vulnerable is the information? Assess the nature and size of asset vulnerability to the five main threats (destruction, modification, disclosure, denial and fraud).

3. What is the cost of losing or compromising the information? The loss of national defense information could disrupt military operations by harming command and control systems.

4. What is the cost of protecting the information? Different types of costs must be considered , such as the unquantified cost of security controls that detract from the user-friendliness of a system, the cost of new equipment, and the financial and administrative cost of recovering information.

Depending on how the above questions are answered, an organization will need to balance the value of the information against the risk of losing it and the financial cost of protecting it.

III.   DOD SECURITY ENVIRONMENT

A.   INTRODUCTION

This chapter is an overview of the Department of Defense Security environment. It explains some of the problems DOD confronts with its current information systems.

B.   DOD INFRASTRUCTURE

DOD has an extensive infrastructure of computers and networks to protect. DOD is faced with the monumental problem of protecting over two million computers, ten thousand local networks, one hundred long-distance networks and over two million Defense computer users and an additional two million non-defense users [Stillman, Stephenson 96].

Because of the rapid growth in computer technology, DOD has become extremely dependent on automated information systems. These systems are inter-connected world-wide. In order for DOD to communicate and exchange unclassified information, commercial carriers and common user networks are utilized. Although this environment offers DOD increased connectivity and seamless information transport, it also increases the risk of unauthorized users accessing sensitive and classified information. Sensitive information includes commercial transactions, payrolls, research data, operational plans, health records and personnel records. Classified information is usually safer from attack than unclassified information, because computers containing this information are isolated from outside networks, data are encrypted and secure circuits are used.

C.   INTERNET

The Internet is a global network interconnecting thousands of dissimilar computer networks and million of computers worldwide. The Internet strives to be a seamless web of networks. It is very difficult to discern where one network ends and another begins. DOD uses the Internet to exchange electronic-mail (e-mail), log on to remote computer sites and upload files from remote locations. During the Persian Gulf conflict, the Department of Defense used the Internet to communicate with United States allies, gather and disseminate intelligence, and counter-intelligence information. The Internet is even viewed as a back-up communications medium [Stillman, Stephenson 96]. Internet connectivity offers numerous advantages to DOD, but it also offer significant security risks. DOD computers are usually attacked in three ways: electronic mail, password cracking, and packet sniffing.

There are several services associated with TCP/IP (Transmission Control Protocol/Internet Protocol) and the Internet. The most commonly used service is electronic mail (sendmail) is used for sending and receiving electronic mail. Sendmail is a UNIX program. UNIX is not a single operating system, but is a family of related operating systems form various companies that have a common heritage and functionality. UNIX computers act as servers to other client operating systems such as MS DOS and Windows NT. The Computer Emergency Response Team Coordination Center (CERT/CC) has published a security problem in sendmail that affects all versions up to and including sendmail 8.7.5.

The sendmail vulnerability permits unauthorized remote program execution. Anyone with access to an account on the system can run programs or write files as the default user. The danger in this is that on many systems the line printer spool director is owned by daemon. Because the line printer subsystem runs 'setuid' root, it may be possible to gain additional privileges. Since sendmail is executing at the system's root level, it has all system privileges and can enter a new password into the system's password file which gives the attacker total system privileges. Solutions to this problem are: install a patch from the vendor; upgrade to the current version of sendmail (8.7.6); or use a program that limits the programs that can be run as the default user.

More recently CERT has issued a warning about a software hole that has been found in the Berkeley Internet Name Daemon (BIND). BIND translates Internet name addresses into numeric addresses [Harreld 97]. BIND is found on all UNIX servers and many NT servers. The hole could be used by attackers to corrupt or capture information the network. The attacker could actually divert traffic to themselves by exploiting this vulnerability. This security hazard can be fixed by plugging the hole with the updated version of BIND (version 8.1.1) [Harreld 97].

Password cracking is a procedure whereby attackers try to guess or steal passwords to obtain access to computer systems. Attackers either try to guess legitimate passwords themselves or use a computer to systematically do the guessing. But the above technique is unnecessary, if the attacker can create his own passwords in a system by exploiting the sendmail vulnerability. Password crackers can be foiled by the use of a good password. Passwords should be used that are not words, different for different

machines. Long passwords with a mix of alphabetic and numeric characters should be used. The best passwords contain a mixed uppercase and lowercase letters, as well as numbers.

Packet sniffing is a software program installed at remote network switches or host computers that monitor information packets as they are routed on the network and sends a copy of the retrieved information to the attacker. Attackers can learn passwords and user identifications by this method.

To ensure password security, a user should not record his password on-line or send it anywhere via electronic mail and do not keep passwords that may have come with your system. Attackers use their unauthorized access to steal information, deny service to authorized users and corrupt data. DOD systems are attractive to attackers because of the financial gain that can be achieved or political reasons (cause harm to particular organizations). Computer attacks, such as the following, are serious threats to the operations of DOD. Some operations could be crippled if supporting technology failed or if information was stolen or destroyed [Stillman, Stephenson 96].

1. Defense could not deliver supplies promptly without a properly functioning inventory and logistics systems.

2. DOD's ability to pay, assign, move, or track people would be severely hampered without globally networked information.

3. DOD's ability to pay vendor, let or track contracts, allocate or release funds would be severely hampered.

4. Simulators that emulate complex battle situations-- to train staff would be affected.

D.   ATTACKS ON DOD

Defense Information System Agency (DISA) estimates that DOD experienced about 250,000 attacks last year [Stillman, Stephenson 96]. Attacks on DOD's computer systems have been costly and has caused considerable damage. Entire networks and systems have been shut down. The attacks are estimated to have cost tens or even hundreds of million of dollars per year [Stillman, Stephenson 96]. The costs include: detecting and reacting to attacks, repairing systems, and checking to ensure the integrity of information; loss of productivity due to computer shut downs; tracking, catching and prosecuting attackers; and the cost and value of information compromised.

Preventing unauthorized users from compromising the confidentiality, integrity, or availability is an enormous task for DOD, because of its increased reliance on outside networks. Tradeoffs must be made between the threat, the value of the information and the cost of protecting it. Although it may not be possible for DOD to anticipate all possible vulnerabilities, steps can be taken to improve DOD's security environment. Strengthening computer security policies and procedures , security training and staffing and detection and reaction programs will go a long way in making it more difficult for attackers.

Defense officials believe that a large part of the Department's security problems result from poorly designed systems or the use of commercial off-the-shelf (COTS)

computer hardware and software products that have little or no inherent security

[Stillman, Stephenson 96]. Chapter four examines one of these COTS software products

(Windows NT) to determine what security problems it may have.

IV.   WINDOWS NT SECURITY ISSUES

A.   INTRODUCTION

This Chapter details the vulnerabilities and threats found in Windows NT. Some of these issues are unique to Windows NT while others are security issues for all operating systems.

B.   TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL (TCP/IP)

TCP/IP governs how data passes between networked computers. It is the most widely used suite of protocols for interconnecting computers and is used on the protocol of the global Internet.

A number of TCP/IP services are not secure and can be used by malicious users to attack networks. Local area networking services used to improve network management are particularly vulnerable to attack. Many sites are unintentionally configured for wide-open Internet access without regard for the potential for abuse from users of the Internet. Quite a few networks permit more TCP/IP services than is required for operations and do not attempt to limit access to information about network computers that could prove valuable to intruders. Although TCP/IP is very flexible, it is difficult to administer correctly. Controls that are accidentally miss-configured can result in unauthorized access.

1.   NetBIOS Over TCP/IP (NetBT)

A name resolution service for Windows NT is NetBT [Strebe, Perkins, Chellis]. NetBT is the session layer network service that performs name-to-IP address mapping for name resolution. Windows NT implements NetBT through the broadcast name resolution and Windows Internet Name Service (WINS). Registration and resolution are two important features of the related naming activities. Registration is the process used to register a unique name for each computer. Resolution is the process used to determine the specific address for a computer name [MS Press 97].

The network menu on Windows NT will support networking over several transport protocols: NetBEUI, IPX/SPX and TCP/IP. NetBIOS Extended User Interface (NetBEUI) is a simple network layer transport developed by Microsoft and IBM which is used for communicating within a single Microsoft network. NetBEUI is not routable. IPX/SPX is a routable network protocol developed by Novell for its NetWare product. NetBIOS is a session layer protocol developed by IBM for its local area networks. NetBIOS over TCP/IP is routable, capable of print and directory sharing and allows remote administration. An attacker could connect to a drive and edit a registry across the Internet using the mapping file LMHOSTS.

To prevent an unauthorized user form taking advantage of this vulnerability, NetBIOS over TCP/IP should be disabled. To unbind the NetBT protocol the user should double click on Network in the Control Panel, select the Bindings tab, show the binding for protocols, then select NetBIOS over TCP/IP binding and click disable.

C. FILE TRANSFER PROTOCOL (FTP)

The file transport protocol (FTP) is one of the protocols that make up TCP/IP suite of protocols. FTP allows users to transfer files from on computer to another. FTP is automatically installed when Windows NT is installed. The home directory specified for FTP service is only the initial current directory. FTP users can change their current directory. FTP users are able to access the root directory of a Windows NT FTP server even though the default directory for the FTP server is not the root directory. This can happen because the path to parent directories are not disabled by FTP server. Specifying a default directory in FTP server only states which directory FTP clients will default to when logged in, but does not disable the path to parent directories. Normal NTFS permissions will apply to whatever account the FTP server user is running under. To prevent users from seeing the root directory of the primary partition, the administrator should create a separate partition for FTP and then configure FTP so that it can only read and /or write to that partition. Also, NTFS can be used to assign directory rights for accounts that will use the Windows NT FTP server.

D. SERVER MESSAGE BLOCK (SMB)

The Server Message Block (SMB) allows remote access to shared directories, the registry, and other system services. The SMB session level access is controlled by username and password.

Users are identified to a system by a Security Identifier (SID). Security identifiers are unique, because when they are created information from the domain, user, time and date is used to create the variable-length hierarchical number [Chacon 97]. There are many types of SIDs. One of the most common SIDs that is present in all NT systems is the dynamic group Everyone. The Everyone group applies to domain users and to members of any trusted domains. The Everyone group cannot be deleted or disabled; it is the default permission group granted to any resource when it is shared [Strebe, Perkins, Chellis 97]. The Everyone group controls the different permission and privileges users may have for accessing the same resource directly at a machine or from across the network. Guest users are members of the Everyone group. The Guest accounts do not have a password in Windows NT. A guest is someone given guest privileges or anyone who failed to log on properly to a Windows NT computer or domain. If users are allowed access to resources via the Everyone group, and the Guest Logon is enabled, then an unauthorized user will have access to everything on the shared resources.

The solution to this problem is: the Administrator should delete the Everyone permission and assign permissions to other groups to prevent global access to shared resources; the Administrator should not leave guest groups enabled; and he should disable access to SMB services from the Internet.

E. REMOTE REGISTRY ACCESS

All the initialization and configuration information used by Windows NT is stored in the Registry. The Windows NT registry is a database repository for information about

22

a computers configuration [MS Press 96]. A key is a folder that appears in the left pane of a Registry Editor window. Keys in the Registry can be altered directly using the Registry Editor.

The Registry Editor can be used to view and change the contents of another computer's Registry if the Server service on the remote computer is running. An unauthorized user could modify keys or assign new value entries to keys. A malicious user could use the Registry vulnerability to deny services to legitimate users by changing Registry entries to make services function strangely so clients are not able to use them. Attackers could also use this vulnerability to break-in and give himself administrative privileges, if the account is an Administrator account.

To protect the Registry, access through the Windows NT Explorer should be restricted. Files stored on the NT file system (NTFS) should be secured by assigning permissions for the Registry Editor and assigning access rights to registry keys. Permissions should be set to specify the users and groups that can have access to registry keys and all unnecessary user and groups should be removed from the list of users or groups authorized to access the Registry keys. Caution should be exercised when changing permissions to limit access to a Registry key because access permission could be denied on a key (folder) needed for configuration by the Network option in the Control Panel [MS Press 96]. This particular vulnerability can countered by disabling Remote Registry Access. Denying access to the Network group will 'Unshare' the entire Registry. By default the Everyone group is given write access to much of the Registry when Windows NT is installed. How much Registry write access is given can be determined by

using the Somarsoft DumpAcl program. The program produces a report of permissions for group files and directories.

F.   PERMISSIONS SET IMPROPERLY

Permissions define what operations can be performed on objects [MS Press 96]. When a user logs on he is given an access token, which identifies which user account is being use and which groups the user is a member of. When a user attempts to access a file, the access token is compared with entries in the files access control list (ACL). If the user has sufficient permissions to access the file, then the user is allowed to perform the action.

Files inherit the security attributes of the directories that contain them when they are created and users inherit permissions based on their group memberships[Strebe, Perkins, Chellis 95]. When files are copied (created) they inherit the security permission of the directory, but when files are moved they retain their original permissions unless they are moved between volumes. A copied file is created in a new location, where it inherit the permissions of the directory it is copied to. With moves, file directory entries are changed to reflect the new location. Files can receive permissions the user did not intend, if the user does not understand the move and copy functions. A user might use the move to place a file into a directory where he is the only one with write permission. However, the file will retain the permissions of the original directory since it was not copied.

The Somarsoft DumpAcl program can make it easy for users to spot files with incorrect permissions. The Somarsoft program causes Windows NT to dump the

permissions (ACLs) for the file system, registry shares and printers in a concise, readable listbox format, so that "holes" in system security are readily apparent.

G.   SECURING A SHARED WORKSTATION

Many organizations (DOD, universities) share workstations. Users want to be able to prevent other users, sharing the same workstation, from accessing their files, while others just want to keep random passersby from using the machine. Share permissions control how access to a shared resource is managed [MS Press 96]. There are several steps that can be taken to prevent inadvertent changes by users and to deter deliberate tampering.

1. Identification and Authentication: Users must uniquely identify themselves by typing a unique log on name and password before they are allowed to access the system.

2. Passwords: The use of a password is mandatory in order to log on to an NT workstation. All passwords used should be difficult to guess. In particular, make sure the administrator password is long, mixed case and alphanumeric.

3. Access Control: Users should log off a workstation completely or lock the workstation when it is unmanned. This can be accomplished by pressing the CTRL-ALT-DEL keys simultaneously and by selecting either the Logoff or Lock workstation buttons.

4. NTFS file security: NTFS provides security and access control for user data files. You can limit access to portions of a file system for specific users and services by using NTFS. The NT file system apply access-control lists (ACLs) to files and directories. NTFS also logs all changes to the file system and can redo or undo every file or directory

update to correct discrepancies stemming form system failures or power losses [Strebe, Perkins, Chellis 97].

Precautions should be taken with computer hardware and software to protect against theft. This includes using cipher or key locks, securing the workstation to the desk, and securing the system unit so that it cannot be opened.

H.   ACCESS VERSUS SECURITY

The Windows NT network environment allows security to be flexible. When applying security in a network environment certain trade-offs may have to be taken. A client/server network is identified in Figure 1. Establishing maximum security on a Windows NT Server that is accessed by Windows NT Workstation clients, limits access to server resources and makes it harder for users to work with the protected resources. It also takes extra effort on the Administrators part to set up and maintain security protections. For example, if only users in the Accountant group are allowed to access financial records, and a new person is hired to do that job, the Administrator has to set up an account for the new person and add that account to the Accountant group. If the new account is created but not added to the Accountant group, the new person cannot access the financial records, ergo cannot perform his job. If security is too restrictive, users will attempt to bypass the security measures established. For example, if the password policy only except extremely difficult passwords, that are hard to remember, users will write them down to avoid being locked out.

Computers are used to store sensitive and sometimes valuable information. The information could range from social security numbers to research data. Administrators would want to protect against unintended and deliberate changes to the way the computer is setup. But users need to be able to do their work, with minimal barriers to the resources they need.
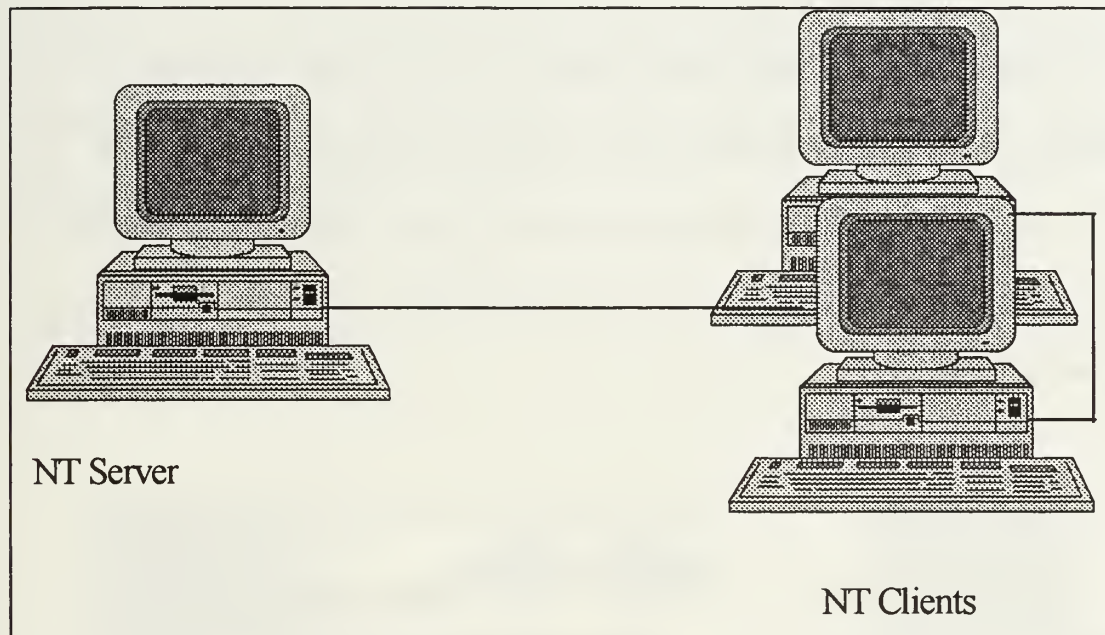
Figure1. Client/Server Network.

I. WORKGROUP VERSUS DOMAIN MODEL

Windows NT uses two security models in the network environment: workgroup and domain. The Workgroup model is a peer-to-peer network. It is a relationship where all devices can act as both a client and server. Each machine in the workgroup maintains its on database of account and security policies. Workgroups are easy to create and are suited for small networks. Table 1 identifies the advantages and disadvantages of the Workgroup model.

Advantages	Disadvantages
Simple design to implement	No central Management
Easy to share resources	Duplicate accounts
Distributed resources	Everybody must be an administrator
Convenient for a limited number	Inefficient for large networks

Table 1. Advantages and Disadvantages of the Workgroup Model.

The Domain model controls the way clients and Windows NT Servers interact in a server-based network. The Windows NT server takes care of security for the network. A client NT workstation retains a local database for the purpose of logging into a computer without logging into the network. Table 2 shows the advantages and disadvantages of the domain model.

Advantages	Disadvantages
Centralized administration	Administration becomes more complex
Centralized access control	Sharing resources becomes more complex
Control of user's environment	Additional administrative overhead
Grouping of resources	Browsing may become a problem

Table 2. Advantages and Disadvantages of the Domain Model.

The domain model allows a finer level of security and network administration. The domain model uses trust relationships to extend access beyond the local domain. A trusting domain allows a trusted domain to access resources in both the trusting and trusted domains. Trusts can be one-way or two-way. Only one domain trusts the other to

authentican users, ergo only users from the trusted domain can have access in both domains. This type of trust is used when all user accounts reside in one domain and resources reside in another domain. Two-way trusts are where both domains trust one another and users from both domains have access in both domains. A trusting domain accepts the authentication or rejection of user accounts from the domain controllers of another domain. Trusted is the domain whose users will have access to both domains. The computer that stores the user and group accounts information and the account and security policies is referred to as the primary domain controller. In Figure 2 arrows point to the users that are trusted.
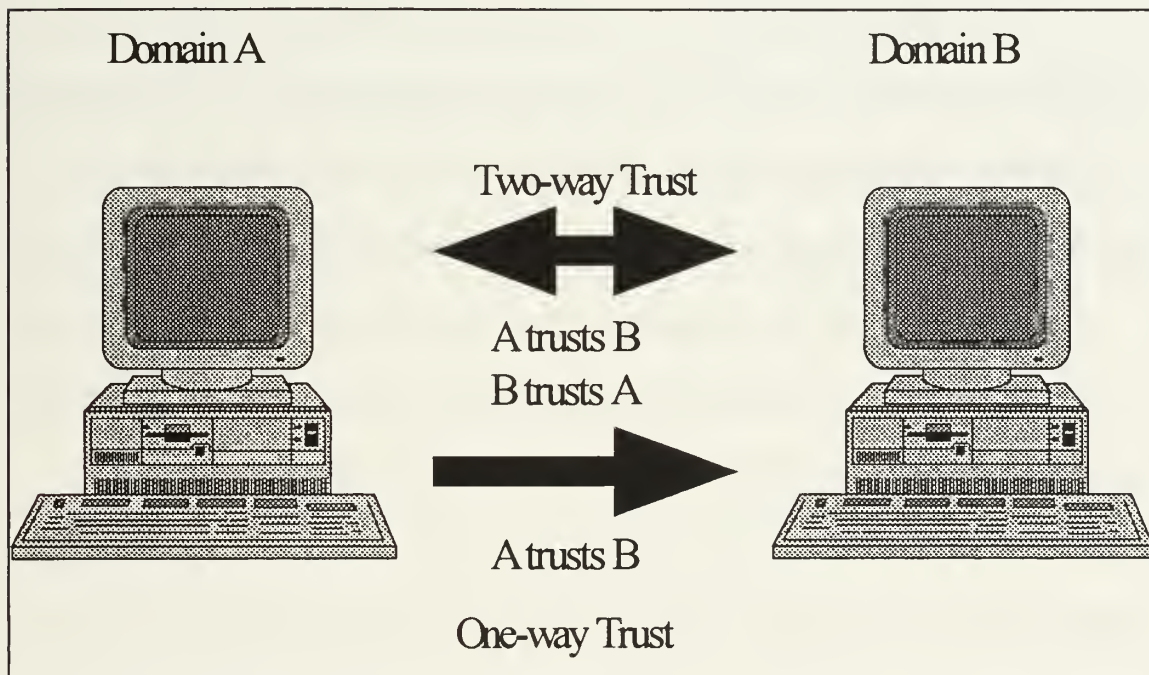

Figure 2. One-way and Two-way Trusts.

V.   SECURING A WORKSTATION

A.   INTRODUCTION

This Chapter provides a security check list for evaluating the security of a Windows NT system. Because different types of information requires different types of security, the need to quantify security or measure it becomes very important.

B.   C2

As computers become increasingly integrated into the way we work and our everyday home life, security becomes increasingly important. The National Computer Security Center (NCSC) is the United States government agency responsible for performing software product security evaluations [MS Press 96]. The NCSC outlines a set of security requirements defined in DOD 5200.28-STD, also known as the Orange Book. The Orange Book classifies systems into four hierarchical categories of increasing security importance--D, C, B, A. The book supplies the criteria for evaluating the effectiveness of security controls implemented in products used in information systems.

"A" is the highest level of security. The "A" security level is reserved for systems providing the most comprehensive security. Division or level "A" derives its security more from design than from security features and functionality. Division "A" requires a formal (mathematical) design and verification[Russell, Gangemi 91].

"B" level is divided into three sub levels: B1 (labeled security protection); B2 (structured protection); B3 (security domains). In division "B", mandatory protection is provided along with discretionary protection.

The "C" level is also divided into two levels: C1 (discretionary security protection); C2 (controlled access protection). In Division "C" users can grant or deny access to other users and groups of users to the system resources.

"D" level systems provide minimal protection. This classification is reserved for systems that are submitted for evaluation and fail. Basic operating systems for personal computers, such as PC's running MS-DOS would probably fall into this category if they were evaluated.

C2 compliance actually applies to stand-alone system security vice network security. According to the Orange Book, workstations that are C2 compliant cannot be hooked into a network. Windows NT is currently under evaluation for networking component of a secure system in compliance with NCSC's "Red Book". The Red Book is an interpretation of the Orange Book as it pertains to network security [MS Press 96].

The following are requirements of C2 level security:

1. The owner of a file or directory must be able to control access to these resources.

2. Once a file is deleted, users must not be able to access any data from that particular file. The system must also protect against the random reuse of objects by other processes.

3. Users must be identified and authenticated by a unique log on and password before they can access the system.

4. Security-related events must be audible by the administrator and access to audited data must be limited to authorized administrators.

5. The system must be able to protect itself against modification of the running system or system files stored on disk.

The evaluation process used by the NCSC does a good job of ensuring a system can enforce an organization's security policy, but it does not dictate what an organization's security policy must be.

C. STANDARD EVALUATION

In this section security settings are outlined. These settings are checked in the User Manager section of a Windows NT system. The User Manager allows individual user accounts and policies to be edited and controlled from a central point.

1. Account Policies and Restrictions

Account policies and restrictions determine how password and log on policies are enforced for the entire domain. The User Manager can be used by the system administrator to set account password expiration and incorrect log on attempts before a user is locked out [MS Press 96].

Password restrictions can be set based on the following password policies:

1. Maximum Password Age: Password should expire in x number of days.

2. Minimum Password Length: Password should have a minimum of six characters.

3. Minimum Password Age: Set to allow changes in x number of days.

4. Password Uniqueness: Set to remember x number of passwords to prevent password reuse.

The Account Lockout option is used to prevent unauthorized users from accessing the system through guessing passwords. The following options should be set to protect against password cracking:

1. Lockout after x bad log on attempts: Set x to 3.

2. Reset Count after x minutes: Set to approximately 30 minutes to avoid unnecessary lengthy lockouts.

3. Lockout Duration field: Set according to Log on policies.

4. Remote users should be forcibly disconnected from server when log on hours expire: This option can be used to prevent after-hour activity or to disconnect systems that were accidentally left on.

5. Users must log on to change password: The Administrator should use this option to prevent users with expired passwords from logging on [Strebe, Perkins, Chellis 97].

2.   User Accounts

Windows NT use the concept of User Accounts to control security and accountability. The log on process connects users to the network. Username and

password identifies and authenticates the user to the network. The following describe properties of the user account that are accessible from the New User dialog box:

1. Account Disabled field prevents users from logging on to the network using the account that has been disabled. This field also allows the account to be placed temporarily out of service.

2. The Account Locked Out field allows the checking of accounts that are locked out due to failed logons.

3. The Groups button field enables the determination of which groups the user belongs to and assigns Group membership.

4. The Profile button field is used to check the location of the user's home directory. This field allows the viewing of the user environment profile information.

5. The Hours button field is used when the administrator wants to evaluate the times that the user can access the network.

6. The Logon To button field is used to evaluate which computers the user can log on to.

7. The Account button field specifies an accounts expiration date.

8. The Dialin button field is used to evaluate dial-in capabilities and it is the button that allows users to dial into a computer using Remote Access Service.

3.   Groups

Windows NT supports two types of groups: Global and Local. Global groups or network groups affect the entire network. Local groups affect only the Windows NT

computer on which they are created [Strebe, Perkins, Chellis 97]. Users who are assigned to groups have all the permission of that group. Use the User Manager option to do the following:

1. The Administrator should check to see if any accounts in a group is inactive so they can be removed.

2. The Administrator should evaluate the members of the Administrators, Server Operators, Account Operators, Backup Operators and Print Operators so all unnecessary accounts are removed.

3. The Administrator should make sure all Administrators use two accounts: one for administrative tasks and one for regular use to avoid accidental changes to protected resources.

4. The Administrator should check files and folders groups have permission to access. This helps in determining whether groups have access permissions they should not have.

5. The Administrator should check to see if local groups hold global groups from other domains to make user that no users have unnecessary access to resources in the current domain.

The membership of groups should be carefully evaluated. A group that is granted permissions to sensitive files might contain users that should not access permission to that material.

4.   The Administrator Account and Administrators Group

The Administrator account and administrators group have unlimited rights on a system. The Administrator account is created by default. This account can never be locked out due to repeated failed log on attempts and is therefore very attractive to hackers who try to break in by guessing passwords [MS Press 96]. The Administrator account manages the overall configuration of the computer and can be used to manage security policies, to create or change users and groups, to set shared directories for networking, and to perform other hardware maintenance tasks [Strebe, Perkins, Chellis 97].

To protect the Administrator account the following should be done:

1. The Administrator should rename the Administrators account to protect the user id of the account from hackers. The default name of the Administrator account is Administrator. The Administrators account can be renamed but it can not be deleted.

2. The Administrator should enable failed logons in the auditing system to detect attempts to log on to the Administrators account.

3. The Administrator should look for unnecessary accounts that have Administrator status to make sure an attacker has not accessed the system and given himself privileges.

4. The Administrator should use separate accounts for administrative activity and general user activity.

5. The Guest Account and Everyone Group

The Guest account should be disabled unless there is a need to allow a specific service to users without passwords. The Guest account allows users with low or no security access to use a workstation. Guest users are members of the Everyone group. If the Everyone group has access permissions to a share and have the Guest Logons enabled, anyone who can access that workstation will have access to everything on that share.

The Everyone group, by default is granted access to your computer from the network [MS Press 96]. The Everyone group can not be deleted or disabled, instead the Everyone permission must be deleted. Permissions can be specifically assigned to other groups to disallow global access to shared resources [Strebe, Perkins, Chellis].

6. User Rights

The User Right policy allows Administrators to control what activity users can have on a specific workstation. Rights apply to the system as a whole, rather than to specific objects, which are controlled by permissions [Strebe, Perkins, Chellis 97].

There are two user rights default settings that should be changed:

1. Logon locally: Allows a user to log on at the workstation, from the computer's keyboard. By default Administrators, Backup Operators, Everyone, Guests, Power Users and Users are assigned this right. The Administrator should change this right to deny Everyone and Guests this right.

2. Shut down the system: Allows a user to shut down Windows NT. By default Administrators, Backup Operators, Everyone, Power Users, and Users are assigned this right. The Administrator should deny Everyone and Users this right.

The Administrator should evaluate all rights to ensure a user has not been granted rights inappropriately.

7.   Files, Directories, Permissions and Shares

Share permissions control how access to a shared resource is managed [Strebe, Perkins, Chellis 97]. The following are share level permissions:

1. No Access: Prevents access to the shared directory regardless of other allowed permissions.

2. Read: Allows viewing of contained files and directories, loading of files, and executing software.

3. Change: Allows all read permissions plus creating, deleting, and changing contained directories and files.

4. Full Control: Allows all change permissions plus changing file system permissions and taking ownership.

On NTFS volumes, permissions can be set on files and folders that tells which groups and users have access to them and the level of access permitted. NTFS file and folder permissions apply both to the users working at the workstation where the file is stored and to users accessing the file over the network when the file is shared [MS Press 96]. Certain actions can be performed on file and folders even if permissions are set on a

file or folder to prevent access to users. If a user has been granted Full Control to a folder, but has been given No Access to a file, the user could still delete the file. The user can do this because he has Full Control rights in the folder. To prevent a user from doing this, permissions must be set on the file itself and set for the folder containing the file [MS Press 96].

When users are members of many groups, some groups may allow him access to a resource while another might restrict his access. Windows NT determines access privileges in the following manner:

1. Administrators always have full access to all resources.

2. A specific denial (No Access permission) always overrides specific access to a resource.

3. When resolving conflicts between share permissions and file permissions, Windows NT chooses the most restrictive [Strebe, Perkins, Chellis 97].

Note that the Everyone group gets full access by default for all new folders that are shared. To prevent this, the Administrator should change the Everyone group's permission for a folder, then any new sub-directories created will get the new permission settings.

8.   Auditing and Event Logs

Windows NT allow the tracking of security events through auditing. The audit shows the action performed, the user who performed it, and the date and time of the

action. Successful and failed attempts can be audited. File and folder access can only be audited on Windows NT File System.

The Event Log records any significant occurrence in the system or an application. The Event Log can help predict and identify the sources of system problems. Events are not audited by default, the Administrator must specify what types of events are audited through the User Manager.

9. Fault Tolerance, Backup, and Uninterruptible Power Supply (UPS)

Fault tolerance is the ability of a system to protect data and allow accessibility in the face of a hardware failure. Use the Disk Administrator utility to check disk systems and use the UPS utility which is located in the control panel to check the status of uninterruptible power supplies.

1. The Administrator should use Disk Manager to make sure disk mirroring or duplexing is taking place. This will provide protection against failed drives and hardware components.

2. The Administrator should make sure the UPS is installed and configured properly. The UPS will protect data on a server that fails from a power loss.

Backup is the process of writing all the data on-line to off-line storage devices. Backup policies and procedures are necessary to ensure essential information is backed up . Since Backup Operators have the ability to access all areas of the system to backup and restore files, they should be carefully evaluated for trustability.

VI. CONCLUSIONS AND RECOMMENDATIONS

A. INTRODUCTION

This chapter draws conclusions about Windows NT security. Recommendations are made concerning DOD's deployment of Windows NT technology, considering its security capabilities.

B. CONCLUSIONS

Windows NT is an operating system designed to take advantage of powerful new desk top systems using processors such as Intel 486 or higher, MIPS R4000 and DEC Alpha. It offers such features as advanced file system, fault tolerance, symmetrical multiprocessing, client/server networking and preemptive multitasking. Both Windows NT workstation and Windows NT server provide preemptive multitasking and support for multiple processors. The primary differences between Windows NT Workstation and Windows NT Server are: Windows NT Server is optimized for network performance, while Windows NT Workstation is optimized for workstation application performance. They are basically the same operating systems with different features enabled.

The National Computer Security Center (NCSC), a division of the National Security Agency (NSA) determined that Windows NT workstation and Windows NT server satisfied the Department of Defense Trusted Computer System Evaluation criteria for a class C2 system. Windows NT was not evaluated for a network environment but was evaluated as a stand-alone product. This of course makes the C2 rating of little use to

DOD. Putting a C2 rating on an unsecured network is inappropriate. Although Windows NT comes with a set of security features, the default setting on the out-of-the box configuration is weak. It is assumed by Microsoft that the average customers may not want a highly secure system on their desk. What does this mean for DOD? DOD is not the average customer. DOD requires a system that can protect valuable and sensitive information. Personnel acting as Administrators will have to be well versed in the installation requirements of Windows NT in order to configure Windows NT for security. Administrators who are not well trained can inadvertently let default settings, such as the Everyone group, remain. The problems associated with the Everyone group were discussed in chapter four of this thesis. The Software Engineering Institute's Computer Emergency Response Team attribute 80% of DOD's security problems to the lack of DOD personnel awareness of security risks and training. Many users do not understand the technology they are using, the vulnerabilities in the network environment, and their responsibility in protecting it. It is not uncommon for DOD to assign the job of maintaining a systems security as a collateral duty.

C.   RECOMMENDATIONS

While it is recognized it is impossible to secure any system completely, there are measures that can be taken to lessen a system's vulnerabilities to threats.

1. DOD should require training in security of personnel who are responsible for managing and securing systems at various defense installations.

2. Develop policies for preventing, detecting, and responding to attacks on DOD systems.

3. Ensure that commercial products address the security needs of DOD, such as having the default settings configured in their most secure mode.

4. DOD should reevaluate NT security on a network basis.

LIST OF REFERENCES

Abrams, M. D., Jajodia, S., Podell, Harold, J., *Information Security, An Integrated Collection of Essays*, IEEE Computer Security Press, Los Alamitos, California 1995.

Bace, R., and Schaefer, M., *TSUPDOOD? Repackaged Problems for You and MMI*, National Security Agency 9800 Savage Road, Fort George Meade, Maryland 20755-6000, IEEE April 1995.

Chacon, Michael, *A Matter of Security*, NT Insider, Microsoft Certified Professional Magazine, July/August 1997. Available at *www.mcpmag.com*

Fites, P., and Kratz, M. P., *Information Systems Security, A Practitioner's Reference*, Van Nostrand Reinhold, 115 Fifth Avenue, New York, New York 1993.

Harreld, Heather, *Feds Urged to Plug Software Hole in UNIX, NT Servers*, Federal Computer Week, Volume 11, Number 26, August 25, 1997.

Microsoft Press, *Microsoft Windows NT Workstation Resource Kit*, Microsoft Press, One Microsoft Way, Redmond, Washington 1996.

Palmer, I. C., Potter, G. A., *Computer Security Risk Management*, Van Nostrand Reinhold, 115 Fifth Avenue, New York, New York 1990.

PCNS Service Company, *Glossary of Network Terms*, Blackfoot, Idaho. Available at *http://www.pcns.net/internetterms.html*

Russell, D., Gangemi Sr., G. T., *Computer Security Basics*, O'Reilly and Associates, Inc., 103 Morris Street, Suite A, Sebastopol, California 1992.

Stillman, R. B., Stephenson, J. B., et al., *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Accounting and Information Management Division, Washington, D. C. May 1996. Available at *http://nsi.org/Library/Compsec/infosec.txt*

Strebe, M., Perkins, C., Chellis, J., *MCSE: NT Server 4 Study Guide*, SYBEX Inc., Marina Village Parkway, Alameda, California 1997.

U. S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA-TCT-606, (Washington, D. C.: U. S. Government Printing Office, September 1994).

APPENDIX

ABBREVIATIONS AND DEFINITIONS

The following listing of abbreviations and definitions is an abridged version of PCNS's terms and acronyms. The abridgement is based on terms used in this thesis. The entire glossary can be found at *http://www.pcns.net/internetterms.html*.

Access Method: Technique for moving data between main storage and input/output devices. In a Systems Network Architecture (SNA) environment, it is the software that controls the flow of information in a network.

Address: Identifier assigned to networks, stations and other devices so that each device can be separately designated to receive and reply to messages.

Address Resolution Protocol (ARP): Internet protocol that dynamically maps Internet addresses to physical (hardware) addresses on local area networks. ARP is limited to networks that support hardware broadcast.

Advanced Program-to-Program Communications (APPC): Part of the SNA protocol that establishes the conditions that enable programs to communicate across the network. This capability, involving LU6.2 and its associated protocols, allows communication between two or more processes in an SNA network without the involvement of a common host system or of terminal emulation.

Advertising: Process by which services on a network inform other devices on the network of their existence. The NetWare network operating system uses the Service Advertising Protocol to do this.

Agent: The part of a networked system that performs information preparation and exchange on behalf of a software entity.

Alarm: Audible or visible warning signal that tells a network administrator that an error has occurred or there is a critical situation on the network.

Alert: Sent by management devices to management consoles to inform administrators of thresholds reached and other discrepancies on the network.

Algorithm: A prescribed set of well-defined rules or processes for arriving at a solution to a problem.

American National Standards Institute (ANSI): ANSI is responsible for the establishment of many standards, including a number of data communications and terminal standards. ANSI is the recognized U.S. representative within CCITT and ISO. See also CCITT and ISO.

American Standard Code for Information Interchange (ASCII): A 7-bit code, intended as a U.S. standard for the interchange of information among communications devices.

Application: A software program or program package that makes calls to the operating system and manipulates data files, thus allowing user to perform a specific job (such as accounting or word processing).

Application binary interface (ABI): A specification defining the interface between an operating system and a certain hardware platform, particularly the calls between applications and the operating system.

Application Interface: A set of software routines and associated conventions that permits application programmers to use that interface as a part of any application.

Application Server: A server in a client-server network which runs one or more applications that can be shared by client stations and which also shares the data processing burden with client stations.

Architecture: The manner in which a system, such as a network, computer or program is structured.

Archive: To create a redundant copy of computer file data, typically to create a backup copy of that data to protect it if the original copy is damaged or otherwise irretrievable. By some definitions, an archive is required to contain copies of every version of a particular file. In this case, to archive means to save a copy of every object in a file system with a separate copy of all changes made to that file. In addition to protecting files from loss, this approach also permits any previous version of a file to be restored, typically by date and time.

ARCnet (Attached Resource Computing Network: A proprietary token-bus networking architecture developed by Datapoint Corporation in the mid-1970s. Currently, ARCnet is widely licensed by third-party vendors and is a popular networking architecture, especially in smaller installations. It is relatively fast (2.5 Mbit/s) and reliable, and it supports coaxial, twisted pair and fiber optic cable-based implementations.

Attach: To access a network server; particularly to access additional servers after logging

in to one server. attributes A technique for describing access to and properties of files and directories within a filing system. For NetWare files, attributes include Read, Write, Create, Delete and Execute Only (prevents files from being deleted or copied). For NetWare directories, attributes include Read, Write, Create, Execute and Hidden (hides information about the directory from file listings, preventing unauthorized access, deletion or copying).

Auto Authentication: In a client-server environment, a utility that lets users access unrestricted network resources without password verification. Only when a user attempts to access a restricted resource does the utility prompt for a password.

Autologin: In a network environment, a utility that regulates user login attempts.

Basic Input/Output System (BIOS): A set of programs, usually in firmware, that enables each computer's central processing unit to communicate with printers, disks, keyboards, consoles and other attached input and output devices.

Berkeley Software Distribution (BSD): A UNIX operating system version developed at the University of California, Berkeley.

Boot: Hard disk drives, floppy diskettes, and logical drives (partitions) all have boot sectors where critical drive information is stored.

Bootsec (Boot Sector or MBR Virus): A virus which infects the boot sector of a fixed or floppy disk. Any formatted disk (even one that is blank, or only contains text data, for example) may contain a boot sector virus. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. This type of virus will place a copy of itself on the boot sector of the hard drive. Every time you boot your system from that point on, you will have the virus active in memory. These are the most common viruses. Any attempt to disinfect these viruses while a virus is active in memory will be defeated since it will re-write itself to the disk as soon as you remove it. Additionally, many of these are stealth viruses. For safety's sake, you should always attempt to disinfect these viruses after a cold boot to a write-protected diskette.

Broadcast: Packet delivery service in which all nodes on a network receive a copy of any frame that is designated for broadcast or, when used as a verb, sending the message to all nodes.

Central Processing Unit (CPU): Main processing unit of a computer.

Channel: Path for transmitting electromagnetic signals; synonym for line or link.

Client: Node or workstation (computer) on a computer network that requests services

from a network server.

Client-Server Network: A network consisting of client nodes (workstations) which have client capabilities only and server nodes which have (usually) server capabilities only.

Client-Server Operating System: An operating system which runs on a server in a client-server network and which is responsible for coordinating the use (by clients) of all resources available from that server.

CMOS: Complimentary Metal Oxide Semi-Conductor. Critical configuration information is stored in CMOS. Some viruses attempt to alter this data.

Connectivity: The ability to connect to and communicate with multiple architectures on a single network.

Data: Data are entities that convey meaning. Computer data is stored as a series of (electrical) charges arranged in patterns to represent information. In other words, data refers to the form of the information (the electrical patterns). It is not the information itself.

Data Encryption Standard (DES):   A standard encryption technique that scrambles data into a code for transmission over a public network.

Decryption: Unscrambling or decoding of encrypted data.

Dedicated: A device that has only one function. For example, a dedicated server cannot be used as a workstation. See also nondedicated.

Dial-Up Line: Communications line accessible via dial-up facilities, typically the public telephone network. See also dedicated line.

Directory Rights: Restrictions specific to a particular directory.

Directory Services: Network service that provides information about an entity of interest.

Disk Duplexing: NetWare feature that protects data from failures in network hardware. In disk duplexing, all data on one hard disk is duplicated on a second hard disk on a separate channel. Disk writes made to the original disk are also made to the second disk. If the original disk or channel fails, the duplicate disk takes over automatically.

Disk Mirroring: NetWare feature that protects data from failures in network hardware. In disk mirroring, all data on one hard disk is duplicated on a second hard disk on the

same channel. Disk writes to the original hard disk are also written to the second hard disk. If the original disk fails, the duplicate disk takes over automatically.

Distributed Application: An application that operates in a distributed computing environment, where application modules may run on different systems.

Distributed Computing: A computer operating environment that may involve computers of differing architectures and data representation formats that share data and system resources.

Distributed Network: A computer network on which processing is shared by many different parts of the network. Processing may be shared by client (local) computers, file servers, print servers and application servers such as database servers. Distributed processing enables the most efficient use of processing power because available processors can be dynamically assigned as either general or job specific processors, depending on the type of work to be done and the existing work load. Distributed processing also enables duplication and distribution of key services, such as directory services, so that full services remain available regardless of the failure of individual parts of the network.

Distributed Processing: A technique to enable multiple computers to cooperate in the completion of tasks, typically in a networked environment. Each computer that contributes to the completion of the total task actually does so by completing one or more individual subtasks independently of its peers, reporting the results from its subtasks as they are completed.

Domain: In the Internet, a part of a naming hierarchy. Syntactically, an Internet domain name consists of a sequence of names separated by periods. In the NetWare network operating system and OSI, it is generally used as an administrative partition of a complex distributed system.

Domain Name System (DNS): Distributed name/address database used on the Internet.

DOS (Direct Operating System): A generic term to refer to those operating systems that use commands rather than having a graphical user interface. The most common of these are DR DOS, MS-DOS and PC DOS.

E-mail (electronic mail): A method of file transfer and message sending among workstations.

Encryption: Scrambling or coding of data for security.

Error Detection: Process of determining whether one or more bits have changed from a

one to a zero, or vice versa, during transmission.

Extended Binary Coded Decimal Interchange Code (EBCDIC): Eight-bit code defined by IBM. Includes values for control functions and graphics.

File Allocation Table (FAT): A FAT keeps track of file locations in a particular volume. The NetWare network operating system (NOS) divides each volume into blocks and stores files on the volume in these blocks. If the file consists of one or more blocks, the file may be stored in blocks that are not adjacent. The FAT keeps track of the block numbers where different parts of the file are located. To retrieve a file, the NetWare NOS searches through the FAT until it finds the FAT entries and corresponding block numbers for the requested file.

File Sharing: An important feature of networking that allows more than one user to access the same file at the same time.

Gateway: A hardware/software package that runs on the OSI application layer and allows incompatible protocols to communicate; includes X.25 gateways. Usually connects PCs to a host machine, such as an IBM mainframe.

Gigabyte (GB): A unit of measure for memory or disk storage capacity. Ten to the ninth power (one billion) bytes.

Groupware: A type of software that supports concurrent use of objects (such as documents, calendars and spreadsheets) by multiple LAN users.

Hierarchical File System (HFS): Attached to AFP in the Macintosh operating system. It manages files and directories.

High-Level Data Link Control (HDLC): Communications protocol defined for high-level, synchronous connections to X.25 packet networks. Similar in almost all respects to SDLC. See also synchronous.

High-Level Language/Application Program Interface (HLLAPI): Application programming interface designed for use with high-level languages. HLLAPI: See High-Level Language/Application Program Interface.

Host: A computer, attached to a network, that provides services to another computer beyond simply storing and forwarding information. Usually refers to mainframe and minicomputers.

Hot Fix: NetWare feature that protects data from failures in network hardware. When the Hot Fix feature is activated, a small portion of a hard disk's storage space is set aside as a Hot Fix redirection area.

Hypertext: A method for storing, retrieving and presenting information based on the processing power of computers. Allows computerized linking and almost instantaneous retrieval of information based on a dynamic index.

Institute of Electrical and Electronic Engineers (IEEE): Creates networking standards for cabling, electrical topology, physical topology and access schemes.

Integrated Services Digital Network (ISDN): A CCITT standard that covers a wide range of data communications issues but primarily the total integration of voice and data. Already having major effects on exchange and multiplexer design.

Interface: Point at which a connection is made between two elements so that they can work together.

International Standards Organization (ISO): Based in Paris, this organization develops standards for international and national data communications.

Internet: Collection of networks and gateways that use the TCP/IP suite of protocols. Lowercase, it is an abbreviation for internetwork.

Internetwork: Two or more networks connected by an internal or external router.

Internetwork Packet Exchange (IPX): A protocol that allows the exchange of message packets on an internetwork.

Interoperability: Ability for devices on a heterogeneous network to transmit and share data.

Kernel: The core of an operating system that is responsible for managing system resources.

Kilobits Per Second (kbit/s): Unit of measure for data transfer rates; two to the 10th power (1,024) bits per second.

Kilobyte (KB): A unit of measure for memory or disk storage capacity; two to the 10th power (1,024) bytes.

Kilobytes per second (kbyte/s): One thousand twenty-four bytes per second. Unit of measure commonly used for transfer rates to and from peripheral devices.

Local Area Network (LAN): A system that links computers together to form a network, usually with a wiring-based cabling scheme. LANs connect personal computers and electronic office equipment, enabling users to communicate, share resources such as data storage and printers, and access remote hosts or other networks.

Logic: A logic bomb is a program which will execute a pre-programmed routine (frequently destructive) when a designated condition is met. Logic bombs do not make copies of themselves.

Login Script: A set of instructions that directs your workstation to perform specific actions when you log in to the network. The network supervisor can create a system-wide login script (which is the same for all users on the network) that instructs all workstations to perform the same actions upon login. Your individual login script executes after the system-wide login script. It specifies your individual drive mappings.

Macro: A macro virus is a virus written in one of the many macro languages. The macro viruses spread via infected files, which can be documents, spreadsheets, databases, or any computer program which allows use of a macro language. At present, these viruses can infect Microsoft Word and Lotus Ami Pro documents.

Mainframe Computer: A large-scale computer (such as those made by Burroughs, Control Data, IBM, Univac and others) normally supplied complete with peripherals and software. Also called a host or CPU. Contrast with minicomputer and desktop computer.

Media: Plural of medium. Physical paths over which communications flow, such as copper wires, coaxial cable or optical fiber.

Megabits Per Second (Mbit/s): Unit of measure for data transfer rates; two to the 20th power (1,048,576) bits per second.

Megabyte (MB): A unit of measure for memory or disk storage capacity; two to the 20th power (1,048,576) bytes.

Message: Logical grouping of information at the application layer.

Message Handling Service (MHS): Novell's store-and-forward technology for sending electronic mail messages.

Minicomputer: A small-scale or medium-scale computer (such as those made by Data General, DEC, Hewlett-Packard and others) that usually services dumb terminals. Contrast with mainframe computer and desktop computer.

Modem: Literally modulator/demodulator. Converts digital data into analog (waveform) signals for transmission along media that carry analog signals and converts received analog signals back into digital data for use by the computer. With the advent of digital lines, there is a also a new kind of modem, called a digital modem, that doesn't actually modulate or demodulate signals but is merely responsible for

their transmission over digital lines.

Multicast: Special form of broadcast in which copies of the packet are delivered to multiple stations, but only a subset of all possible destinations.

Multiple Name Space Support: The method that allows various workstations running different operating systems to create their own familiar naming conventions. Different operating systems have different conventions for naming files, but with multiple name space support, the name spaces supported on a volume are configurable so that each file on a given volume has a name that any workstation can recognize.

Multiple Virtual Storage (MVS): IBM operating system for large host systems.

Multiplexer: Device that allows a single communications circuit to take the place of several parallel ones; often used to allow remote terminals to communicate with front-end processor ports over a single circuit.

Multitasking: The ability to run two or more programs (tasks) on one computer at the same time. The tasks take turns using available I/O and CPU cycles.

Multi-vendor network: Network comprised of components from different vendors.

NetBIOS (Network Basic Input/Output System): A programmable entry into the network that allows systems to communicate over network hardware using a generic networking API that can run over multiple transports or media.

NetWare network operating system (NOS): The network operating system developed by Novell, Inc. The NetWare NOS is loaded on the server when the server is booted; it controls all system resources and the way information is processed on the entire network or internetwork. server.

NetWare UNIX Client (NUC): Software that allows a UnixWare system to behave as a recognized client to NetWare software. The NetWare network operating system provides services to UnixWare users and applications, allowing access to remote directories, files and printers on NetWare servers as if they were local.

Network: A system that sends and receives data and messages, typically over a cable. A network enables a group of computers to communicate with each other, share peripherals (such as hard disks and printers), and access remote hosts or other networks.

Network Adapter: The hardware installed in workstations and servers that enables them to

communicate on a network. See also adapter.

Network Computing: A multivendor computing environment that integrates local and wide area network technologies to provide enterprise-wide connectivity.

Network File System (NFS): A distributed file system network protocol developed by Sun Microsystems.

Node: Device that is connected to a network and is capable of communicating with other network devices. In NetWare, a node is considered to be an end system, such as a workstation.

Nondedicated: A device that performs multiple simultaneous functions. For example, a nondedicated network server runs the network functions and performs as a workstation. See also dedicated.

Open Architecture: An architecture that is compatible with hardware and software from any of many vendors.

Operating System (OS): Software that manages a computer system. It controls data storage, input and output to and from the keyboard and other peripheral devices, and the execution of compatible applications.

OS/2: An operating system that uses a graphical user interface and was designed by IBM.

OSI (Open Systems Interconnection) reference model: A model for network communications consisting of seven layers that describe what happens when computers communicate with one another. packet: The unit of information by which the network communicates. Each packet contains the identities of the sending and receiving stations, error-control information, a request for services, information on how to handle the request and any necessary data that must be transferred.

Passwords: NetWare security feature. Supervisors of NetWare networks have the option of requiring users to use a password when they log in to the network. If passwords are required, all users must have unique passwords. Passwords in the NetWare network operating system are encrypted; that is, they are stored on the server in a format only the server can decode.

Peer-To-Peer communication: Communication directly between devices that operate on the same communications level on a network, without the intervention of any intermediary devices such as a host or server. A peer-to-peer communication method (or protocol) defines only the basic mechanisms used to transfer data; it need not specify when or why peer application programs or nodes interact or how communication between such applications or nodes should be organized in a

distributed environment. The latter problems fall into the domain of the peer-to-peer operating system (see peer-to-peer network below).

Peer-To-Peer network: A network consisting of nodes (computers) which all have both client and server capabilities and on which communication and data sharing is carried on directly between nodes, rather than being arbitrated by an intermediary node. On a peer-to-peer network all nodes run the same peer-to-peer operating system, which gives them both client and server capabilities.

Platform: Term used as a generic reference to all possible choices for some specific part of the computing environment.

Port: For hardware, a connecting component that allows a microprocessor to communicate with a compatible peripheral. For software, a memory address that identifies the physical circuit used to transfer information between a microprocessor and a peripheral.

Protocol: Set of rules that allow computers to connect with one another, specifying the format, timing, sequencing and error checking for data transmission.

Protocol suite: A collection of networking protocols that provides the communications and services needed to enable computers to exchange messages and other information, typically by managing physical connections, communications services and application support.

Queue: A line or list formed by items waiting for service, such as tasks waiting to be performed, stations waiting for connection, or messages waiting for transmission.

Real-Time: An on-line computer that generates output nearly simultaneously with the corresponding inputs. Often, a computer system whose outputs follow its inputs by only a very short delay.

Record Locking: This feature on the network operating system prevents two users from writing simultaneously to the same record.

Redundancy: A duplicate capacity that can be called upon when a failure occurs; having more than one path to a signal point.

Remote Dial-Back: Dials number back to confirm user's number. It is a security method procedure.

Rights: NetWare security feature. Rights control which directories and files a user can access and what the user is allowed to do with those directories and files. Rights

are assigned to directories and files by the network supervisor.

Router: A software and hardware connection between two or more networks, usually of similar design, that permits traffic to be routed from one network to another on the basis of the intended destinations of that traffic.

Sequenced Packet Exchange (SPX): A protocol by which two workstations or applications communicate across the network. SPX uses NetWare IPX to deliver the messages, but SPX guarantees delivery of the messages and maintains the order of messages on the packet stream.

Server: A computer on the network capable of recognizing and responding to client requests for services. These services can range from basic file and print services to support for complex, distributed applications.

Service Advertising Protocol (SAP): A NetWare feature that advertises the services available on the Applications Server.

Standalone: A computer that is not connected to a network.

Store-and-Forward: Message-switching technique in which messages are temporarily stored at intermediate points before being transmitted to the next destination.

Striping: A technique for improving I/O performance by interleaving file systems or data bases across multiple disks.

Supervisor: The person responsible for the administration and maintenance of a network or database. A supervisor has access rights to all volumes, directories and files.

Synchronous: A data transmission mode in which synchronization is established for an entire block of data (message). See also asynchronous.

Synchronous Data Link Control (SDLC): IBM-defined link-control protocol that is code-independent.

System Application Architecture (SAA): A set of IBM-defined standards designed to provide a consistent environment for programmers and users across a broad range of IBM equipment, including microcomputers, minicomputers and mainframes.

System Fault Tolerance (SFT): Duplicating data on multiple storage devices so that if one storage device fails, the data is available from another device. There are several levels of hardware and software system fault tolerance. Each level of redundancy (duplication) decreases the possibility of data loss.

System Network Architecture (SNA): IBM network architecture, defined in terms of its functions, formats and protocols.

TCP/IP (Transmission Control Protocol/Internet Protocol): A protocol suite and related applications developed for the U.S. Department of Defense in the 1970s and 1980s specifically to permit different types of computers to communicate and exchange information with one another. TCP/IP is currently mandated as an official U.S. Department of Defense protocol and is also widely used in the UNIX community.

Telnet: Protocol in the TCP/IP suite that governs character-oriented terminal traffic.

Terminal: A device, usually equipped with a keyboard and display, capable of sending and receiving data over a communications link.

Terminal Emulation: Software that allows a microcomputer to function as a dumb terminal.

Throughput: Net data transfer rate between an information source and an information destination.

Topology: The physical layout of network components (cable, stations, gateways, hubs and so on). There are three basic interconnection topologies-star, ring and bus networks.

Transaction: A specific delimited amount of processing, intended to be an indivisible action.

Transparent: Function that operates without being evident to the user.

Trojan: A Trojan (or Trojan Horse) is a program which carries out an unauthorized function while hidden inside an authorized program. It is designed to do something other than what it claims to, and frequently is destructive in its actions.

Uninterruptible Power Supply (UPS): A backup power unit that provides continuous power even when the normal power supply is interrupted.

UNIX: Operating system developed by AT&T Bell Laboratories. Allows a computer to handle multiple users and programs simultaneously.

User: Any person who attaches to a server or host.

User Accounts: This account determines what name the user uses to log in to the network, the groups the user belongs to and what trustee assignments the user has. User

accounts are maintained by the network supervisor.

VAX: A Digital Equipment Corporation minicomputer.

Virtual: Conceptual or appearing to be, rather than actually being.

Virus: A virus is an independent program which reproduces itself. It may attach to other programs; it may create copies of itself.

VMS (Virtual Memory System): Operating system for DEC VAXs.

Volume: A volume is the highest level in the NetWare directory structure, residing at the same level as a DOS root directory. A volume represents a physical amount of hard disk storage space.

Wide Area Network (WAN): A WAN is two or more LANs in separate geographic locations connected by a remote link.

Workgroup: Two or more individuals on a LAN who share files, databases and other resources.

Workstation: Any individual personal computer that is connected to a network.

Worm: A worm is a program which reproduces by copying itself over and over, system to system. Worms are self-contained and generally use networks to spread.

X.25: A CCITT standard that defines the communications protocol for access to packet-switched networks.

X.400: Open Systems Interconnection (OSI) standard that defines how messages are to be encoded for the transmission of electronic mail and graphics between dissimilar computers and terminals; defines what is in an electronic address and what the electronic envelope should look like. The X.400 standards are a subset of, and conform to, the X.25 standard approved by the Consultative Committee for International Telegraphy and Telephony (CCITT).

X Windows: Standard set of display-handling routines developed at MIT for UNIX workstations; they allow the creation of hardware-independent graphical user interfaces.

INITIAL DISTRIBUTION LIST